



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/610,798      | 07/06/2000  | Suresh Krishna       | BRCMP003            | 4877             |

28393 7590 11/13/2006

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.  
1100 NEW YORK AVE., N.W.  
WASHINGTON, DC 20005

EXAMINER

ORTIZ, BELIX M

ART UNIT PAPER NUMBER

2164

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

|                              |                               |                                |  |
|------------------------------|-------------------------------|--------------------------------|--|
| <b>Office Action Summary</b> | Application No.<br>09/610,798 | Applicant(s)<br>KRISHNA ET AL. |  |
|                              | Examiner<br>Belix M. Ortiz    | Art Unit<br>2164               |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 25 August 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 24-41 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 24-41 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                       | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>8/25/06, 9/25/06</u>  | 6) <input type="checkbox"/> Other: _____                          |

## DETAILED ACTION

### Remarks

1. In response to communications files on 25-August-2006. Claims 24-41 are amended by Applicant's request. Therefore, claims 24-41 are presently pending in the application.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 24-26, 28-32, and 36-41 are rejected under 35 U.S.C. 103(a) (Eff. Filing date of claims benefit application: 9/23/1999) as being unpatentable by Leung (U.S. patent 6,760,444) (Eff. Filing date of application: 1/8/1999 ); in view of Gunter et al. (U.S. patent 6,751,728) (Eff. Filing date of application: 6/16/1999); and further in view of Chang et al. (U.S. patent 6,862,278) (Eff. Filing date of application: 6/18/1998).

As to claim 24, Leung teaches a device, comprising:

a distributor unit in the device that distributes a plurality of packets and security association information associated with the plurality of packets according to a distribution scheme (see figure 1; column 2, lines 57-67; column 3, lines 1-15; and column 7, lines 33-50);  
and

wherein the plurality of security processing engines, receive at least a portion of the security association information associated with the packets (see column 4, lines 32-62; column 6, lines 7-46; column 7, lines 336-50; and claims 1-3), and

Leung does not teach a plurality of security processing engines in the device, coupled to the distributor unit, that perform authentication and cryptographic functions.

Gunter et al. teaches a system and method of transmitting encrypted packets through a network access point (see abstract), in which he teaches a plurality of security processing engines in the device, coupled to the distributor unit, that perform authentication and cryptographic functions (see abstract; figures 1, 3, 5, characters 112 and 116, and 8, character 152; column 1, lines 66-67; and column 2, lines 1-9).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Leung by the teaching of Gunter et al., because a plurality of security processing engines in the device, coupled to the distributor unit, that perform authentication and cryptographic functions, would enable the method because “When the NAP receives such an encrypted packet intended for a host on its intranet, it cannot perform the address translation by simply replacing the original destination address with the intranet address of the receiving host.

This is because the original destination address is used to generate the hash value in the packet. When the receiving host receives the modified packet, it decrypts the encrypted portion and authenticates the packet by calculating another hash value based on the addresses and data in the received packet, and comparing this hash value with the hash value included in the packet”, (see column 1, lines 65-67 and column 2, lines 1-9).

Leung does not teach wherein the plurality of security processing engines process the plurality of packets in parallel.

Chang et al. teaches system and method using a packetized encoded bitstream for parallel compression and decompression (see abstract), in which he teaches wherein the plurality of security processing engines process the plurality of packets in parallel (see column 2, lines 32-39).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Leung by the teaching of Chang et al., because wherein the plurality of security processing engines process the plurality of packets in parallel, would enable the method because “Since each packet has a fixed-length with a tag field for directing, a distributor can efficiently send different packets to different decoder units which can then process the packets in parallel”, (see column 2, lines 32-39).

As to claim 25, Leung as modified teaches wherein the plurality of packets are buffered prior to being processed by the plurality of security processing engines (see Gunter et al., column 3, lines 64-67 and column 4, line 1).

As to claim 26, Leung as modified teaches the device further comprising a classification module that determines security association information %associated with a plurality of packets, wherein the classification module is configured to provide at least a portion of the security information associated with the packets to the distributor unit (see Gunter et al., column 10, lines 19-23 and column 10, lines 33-35).

As to claim 28, Leung as modified teaches wherein the security association information includes a sequence number, an anti-replay window, and a lifetime of the security association (see Leung, column 3, lines 45-67 and column 4, lines 1-4).

As to claim 29, Leung as modified teaches wherein the security association information further includes an encapsulating security payload (ESP) encryption algorithm identifier and one or more ESP encryption keys (see Gunter et al., column 7, lines 33-39).

As to claim 30, Leung as modified teaches wherein the security association information further includes an ESP authentication algorithm identifier and one or more ESP authentication keys (see Gunter et al., column 7, lines 33-39).

As to claim 31 Leung as modified teaches wherein the security association information further includes an authentication header (AH) authentication algorithm identifier and one or more AH authentication keys (see Gunter et al., figure 5; column 2, lines 4-9; and column 8, lines 22-27).

As to claim 32, Leung as modified teaches wherein the security association information includes protocol mode information (see Gunter et al., column 7, lines 10-19).

As to claim 36, Leung as modified teaches wherein the system is a router (see Gunter et al., column 4, lines 44-46 and column 5, lines 48-51).

Art Unit: 2164

As to claim 37, Leung as modified teaches wherein the system is a firewall (see Gunter et al, column 1, lines 32-35 and column 5, lines 34-37).

As to claim 38, Leung as modified teaches wherein the system is a network communication device (see Gunter et al, abstract and column 1, lines 7-11).

As to claim 39, Leung as modified teaches wherein the system is a security gateway (see Gunter et al, column 5, Lines 35-38).

As to claim 40, Leung as modified teaches wherein the system is a server (see Gunter et al, column 1, lines 24-26; column 6, lines 44-49; and column 6, lines 62-64).

As to claim 41, Leung as modified teaches wherein the system is a network line card (see Gunter et al, column 4, lines 14-22).

4. Claim 27 is rejected under 35 U.S.C. 103(a) (Eff. Filing date of claims benefit application: 9/23/1999) as being unpatentable by Leung (U.S. patent 6,760,444) (Eff. Filing date of application: 1/8/1999 ); in view of Gunter et al. (U.S. patent 6,751,728) (Eff. Filing date of application: 6/16/1999); and further in view of Chang et al. (U.S. patent 6,862,278) (Eff. Filing date of application: 6/18/1998) as applied to claims 24-26, 28-32, and 36-41 above, and further in view of Barlow et al. (U.S. patent 6,038,551) (Eff. Filing date of application: 3/11/1996).

As to claim 27, Gunter et al. does not teach wherein the distributor unit and the plurality of security processing engines are on the same chip.

Barlow et al. teaches system and method for configuring and managing resources on a multi-purpose integrated circuit card using a personal computer (see abstract), in which he teaches wherein the distributor unit and the plurality of security processing engines are on the same chip (see column 7, lines 42-45 and column 11, lines 43-53).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Leung by the teaching of Barlow et al., because wherein the distributor unit and the plurality of security processing engines are on the same chip, would enable the system because, in the illustrated embodiment, the IC card 14 is configured with cryptography acceleration circuitry 64, shown integrated with the CPU 50, which streamlines cryptography computations to improve speed (see Barlow et al., column 11, lines 43-47).

5. Claim 33 is rejected under 35 U.S.C. 103(a) (Eff. Filing date of claims benefit application: 9/23/1999) as being unpatentable by Leung (U.S. patent 6,760,444) (Eff. Filing date of application: 1/8/1999 ); in view of Gunter et al. (U.S. patent 6,751,728) (Eff. Filing date of application: 6/16/1999); and further in view of Chang et al. (U.S. patent 6,862,278) (Eff. Filing date of application: 6/18/1998) as applied to claims 24-26, 28-32, and 36-41 above, and further in view of Robinson (U.S. patent 5,734,829) (Eff. Filing date of application: 10/20/1995).



Art Unit: 2164

As to claim 33, Leung does not teach wherein the distribution scheme is a round-robin distribution scheme, wherein the distributor unit selects a next available security processing engine in a round-robin manner.

Robinson teaches a method and program for processing a volume of data on a parallel computer system (see abstract) in which he teaches wherein the distribution scheme is a round-robin distribution scheme, wherein the distributor unit selects a next available security processing engine in a round-robin manner (see column 2, lines 43-51).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Leung by the teaching of Robinson, wherein the distribution scheme is a round-robin distribution scheme, wherein the distributor unit selects a next available security processing engine in a round-robin manner, would enable the system to reduce the throughput time as taught in Robinson (Col. 2, lines 5-9).

6. 9. Claims 34-35 is rejected under 35 U.S.C. 103(a) (Eff. Filing date of claims benefit application: 9/23/1999) as being unpatentable by Leung (U.S. patent 6,760,444) (Eff. Filing date of application: 1/8/1999 ); in view of Gunter et al. (U.S. patent 6,751,728) (Eff. Filing date of application: 6/16/1999); and further in view of Chang et al. (U.S. patent 6,862,278) (Eff. Filing date of application: 6/18/1998) as applied to claims 24-26, 28-32, and 36-41 above, and further in view of Martin (U.S. patent 5,867,706) (Eff. Filing date of application: 12/19/1996).

As to claims 34 and 35, Leung does not teach the device further comprising an order maintenance packet retirement unit and wherein the distributor unit assigns packets for processing to a next available security processing engine regardless of the order received and the order maintenance packet retirement unit outputs the processed packets such that packet order is maintained.

Martin discloses that each processor contains a load determining means that determines activity for the processor and is ultimately used by the decision means to decide which processor should service a client request (Abstract), which meets the limitation of the distributor unit assigns packets for processing to a next available security processing engine regardless of the order received and the order maintenance packet retirement unit outputs the processed packets such that packet order is maintained.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Leung by the teaching of Martin, because the system further comprising an order maintenance packet retirement unit and wherein the distributor unit assigns packets for processing to a next available security processing engine regardless of the order received and the order maintenance packet retirement unit outputs the processed packets such that packet order is maintained, would enable the system "Decision means (90) is then used which, for each reference to a subsequent block of information in the file constructed by the block retrieval means (80), determines, based on the load distribution record, which processor should service a request from the client computer (50) for that subsequent block of information, and includes an address for that processor in the file constructed by the block retrieval means (80)", (see abstract).

*Response to Arguments*

7. Applicant's arguments filed 25-August-2006 with respect to the rejected claims in view of the cited references have been fully considered but they are not found persuasive:

In response to applicants' arguments that Gunter "does not teach a plurality of security processing engines in the device, coupled to the distributor unit, that perform authentication and cryptographic functions", the arguments have been fully considered but are not deemed persuasive, because Gunter et al. teaches cryptographic engines on figures 3, 5, and 8; And "when the receiving host receives the modified packet, it decrypts the encrypted portion and authenticates the packet by calculating another hash value based on the addresses and data in the received packet, and comparing this hash value with the hash value included in the packet", (see Gunter et al., column 2, lines 1-9).

Gunter et al. teaches security processing in the device that perform authentication and cryptographic function, (see Gunter et al., abstract) where he teaches "The intranet address of the receiving host is also included in the packet in the non-encrypted form and is used in the calculation of the cryptographic hash or the like that is included in the packet for authentication purposes. The encrypted packet is then routed to the NAP through the external network. When the NAP receives the packet, it strips the intranet address of the receiving host from the packet and uses that address to replace the original destination address in the packet".

*Conclusion*

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Belix M. Ortiz whose telephone number is 571-272-4081. The examiner can normally be reached on Monday-Friday 9am-5pm.

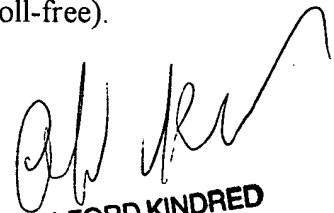
The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2164

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

bmo

November 6, 2006



**ALFORD KINDRED  
PRIMARY EXAMINER**